418 Rec'd PCT/PTO 03 DEC 1999

FORM PTO-1390 (Modified) (REV 10-95) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
RCA88637	
U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	
09/445132	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US98/11633	05 June 1998	06 June 1997

TITLE OF INVENTION

CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES

APPLICANT(S) FOR DO/EO/US

Ahmet Mursit Eskicioglu, Keith Reynolds Wehmeyer and David Emery Virag

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ A copy of the International Search Report (PCT/ISA/210).
8. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 18 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. w/Eight (8) refs + PCT Search Report
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
    A **SECOND** or **SUBSEQUENT** preliminary amendment.
16. ☐ A substitute specification.
17. ☐ A change of power of attorney and/or address letter.
18. ☒ Certificate of Mailing by Express Mail
19. ☒ Other items or information: Return Receipt Postcard

418 Rec'd PCT/PTO 03 DEC 1999

U.S APPLICATION NO. (IF KNOWN, SEE 37 CFR) 09/445132	INTERNATIONAL APPLICATION NO. PCT/US98/11633	ATTORNEY'S DOCKET NUMBER RCA88637

20. The following fees are submitted:.		CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :			
☒ Search Report has been prepared by the EPO or JPO	**$840.00**		
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482)	**$670.00**		
☐ No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))	**$760.00**		
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO	**$970.00**		
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)	**$96.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =		**$840.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).		**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	20 - 20 =	0	x $18.00	**$0.00**	
Independent claims	3 - 3 =	0	x $78.00	**$0.00**	
Multiple Dependent Claims **(check if applicable).**			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$840.00**	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable).**			☐	**$0.00**	
SUBTOTAL =				**$840.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).			+	**$0.00**	
TOTAL NATIONAL FEE =				**$840.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☐	**$0.00**	
TOTAL FEES ENCLOSED =				**$840.00**	
				Amount to be: refunded	$
				charged	$

☐ A check in the amount of to cover the above fees is enclosed.

☒ Please charge my Deposit Account No. **07-0832** in the amount of **$840.00** to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **07-0832** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Joseph S. Tripoli - Patent Operations
Thomson multimedia Licensing Inc.
PO Box 5312, 2 Independence Way
Princeton, NJ 08543-5312

SIGNATURE

David T. Shoneman
NAME

39,371
REGISTRATION NUMBER

12/3/99
DATE

PCT # 13

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Eskicioglu, et al.
Serial No.	:	09/445,132
Filed	:	December 3, 1999
For	:	CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES

ATTENTION: BOX MISSING PARTS

FILING OF MISSING PARTS OF APPLICATION WITH AUTHORIZATION TO CHARGE DEPOSIT ACCOUNT AND CERTIFICATE OF MAILING

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In response to the Notice to File Missing Parts of Application Under 35 USC 371, mailed January 28, 2000, and relating to the above-identified application .

Applicant hereby submits the following and authorizes the following charges:

1) A copy of an executed Declaration and Powers of Attorney

2) A surcharge of $130.00 required under 37 CFR 1.16(e) for filing the Declaration on a date later than the filing date of the application.

3) A copy of Notice to File Missing Parts of Application Filing Date Granted (PTO-1533).

Please charge the cost of the surcharge and any other required fees to Deposit Account No. 07-0832. A duplicate copy of this letter is enclosed for use in charging the deposit account.

Respectfully Submitted,

BY: _____

David T. Shoneman, Attorney
Registration No. 39,371
(609) 734-9586

Thomson Multimedia Licensing Inc.
PO Box 5312, 2 Independence Way
Princeton, NJ 08543-5312

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in a postage paid envelope addressed to: Assistant Commissioner for Patents and Trademarks, Washington, D.C. 20231, Attn: Box Missing Parts on the date indicated below.

Date: 3/9/00

Signature _____

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Ahmet Mursit Eskicioglu et al.

Int'l. Appl. No. : PCT/US98/11633

Int'l. Filing No : 05 June 1998 (05.06.98)

For : CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES

PRELIMINARY AMENDMENT

Honorable Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In the US national phase application of PCT/US98/11633 filed herewith, please enter the following amendments:

Please amend the claims as follows:

In the Claims

11. (Amended) A method [system] for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. The method [system] of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. The method [system] of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. The method [system] of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. The method [system] of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. The method [system] of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. The method [system] of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. The method [system] of Claim 17 wherein said first digital certificate is stored in said smart card.

19. The method [system] of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

20. The method [system] of Claim 19 wherein said second digital certificate is stored in said service provider.

REMARKS

No fee is believed to been incurred by virtue of this amendment. However, if a fee is incurred on the basis of this amendment, please charge such fee against deposit account 07-0832.

Respectfully Submitted,
Ahmet Mursit Eskicioglu et al.

By: _____

David T. Shoneman, Attorney
Registration No. 39,371
(609) 734-9875

THOMSON multimedia Licensing Inc.
PO Box 5312, 2 Independence Way
Princeton, NJ 08543-5312

CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a device, such as a "consumer electronic device". Examples of such consumer electronic devices include separate devices or "boxes" that may be located on top of, and coupled to a television receiver, i.e., set-top boxes.

Background of the Invention

In general, conditional access involves limiting or controlling the communication with a device based on predetermined criteria. Conditional access may be achieved by connecting two devices together when communication therebetween is desired and by disconnecting the two devices from one another when such communication is no longer desired. However, in the context of today's sophisticated computer networks interconnected to form what is known as the world-wide web ("web"), many, if not all, of the devices designed to communicate with the web are "permanently" connected to the web through modem hookups or other means. That is, the devices usually remain physically connected to the web. Typically, access to the web is via a specially designed software package loaded onto a computer and a modem; this software enables a user to connect to an internet service provider who acts as the gate keeper to the web. The user typically pays a monthly fee to the service provider for access to the internet, either on a limited or unlimited basis. The proliferation of users who regularly access the

web as a source of information or even as a means of communicating via E-Mail for both business and personal reasons has created a very competitive market for both service providers and the manufacturers of the necessary hardware. Thus, as one would expect there are numerous service providers, each requiring specialized software for access.

An outgrowth of today's emerging digital consumer electronic products is an opportunity to access the Internet from a user's television. Such access has been accomplished by utilizing the user's television as a monitor or display device in conjunction with a set-top box that provides the software (e.g., a web browser) and hardware (e.g., modem, ethernet, ADSL or any equivalent connection means) needed to interface to the web. For example, the RCA Network Computer manufactured by Thomson Consumer Electronics is such a set-top box that may be connected to both a television and a phone line or the like thereby permitting the user to access the web. Set-top boxes may provide a means for a variety of internet applications (e.g., electronic commerce) from the home, the office or any location without utilizing a personal computer or any general purpose computing device. These set-top boxes have open hardware architectures which would permit easy adaptation of the set-top box thereby permitting use with any of a plurality of service providers.

Summary of the Invention

The manufacturers of these set-top boxes may desire that the box only be used with selected service providers. For example, the manufacturer of the box may be compensated by the service provider

for each connection to the service from the box. Thus, the flexibility of the set-top box's open hardware architecture in combination with a competitive market for such devices necessitates the need to provide a system for providing conditional access in the set-top box so that the box can only connect to selected service providers. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

Generally, the present invention defines a method for managing access to a device by sending a first message to a second device; receiving a digital certificate encrypted using a first private key; receiving the first message encrypted using a second private key; authenticating the second device; and establishing a communication channel between the devices.

In accordance with one aspect of the present invention, the first message comprises data associated with the first device and a date and time stamp, and the digital certificate comprises data associated with the second device and a second public key.

In accordance with another aspect of the present invention, the step of authenticating comprises decrypting the digital certificate using a first public key; decrypting the first encrypted message using the second public key to generate a first decrypted message; and comparing the first decrypted message to the first message.

In accordance with another aspect of the present invention, the method further comprises providing confirmation of

the authentication to said second device by encrypting the first message using the second public key to generate a second encrypted message; and sending the second encrypted message to the second device.

In accordance with still another aspect of the present invention, the digital certificate, the first public and first private keys are issued by an independent certificate authority and are associated with the second device.

In accordance with yet another aspect of the present invention, a system for managing access between a service provider and a set-top box having a smart card coupled thereto, the set-top box sends a first message to the smart card; receives a smart card (first) digital certificate encrypted using a private key; authenticates the smart card; contacts the service provider and sends a second message to the service provider; receives a service provider (second) digital certificate encrypted using another private key; receives the second message encrypted using yet another private key; authenticates the service provider; provides confirmation to the service provider; and establishes a communication channel with the service provider. Particularly, the two messages contain at least set-top box identification data.

In accordance with yet another aspect of the present invention, the smart card includes service provider identification data associated with a plurality of service providers.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawings

Figure 1 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention; and

Figure 2 is a flowchart diagram of an exemplary implementation of the conditional access system of Figure 1.

Figure 3 is a block diagram of an exemplary implementation of the system of Figure 1 wherein any one of a plurality of set-top boxes may communicate with any one of a plurality of service providers.

Detailed Description of the Drawings

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. When implemented within a set-top box, the conditional access system permits the set-top box to authenticate the service provider and/or a smart card used to access services before a communication channel is established. Such a conditional access system may act as a toll bridge for access to services, thereby permitting a mechanism for the manufacturer of the set-top box to collect fees based on use of its set-top box.

In Figure 1, the system 10 for managing access to a set-top box (STB) 20, for example, the RCA Network Computer, is depicted. Smart Card (SC) 30 is inserted into or coupled to a smart card reader (not shown) included in STB 20; an internal bus 25 interconnects STB 20 and SC 30 thereby permitting the transfer of data therebetween. Alternately, the functionality of the smart card may be embedded within the set-top box. STB 20 is connected to service provider (SP) 40 via a dial-up link or a direct link, which is depicted as element 45. Certificate Authority (CA) 50 is not directly connected to either SP 40 or STB 20 but issues digital certificates and public and private key pairs, which are used as explained below. These digital certificates are used by service providers and smart card manufacturers. It is within the scope of this invention that the digital certificates could be provided via an on-line connection. Further, it is within the scope of this invention that the role of Certificate Authority may be performed by SP 40 in collaboration with the manufacturer of the STB 20. The conditional access system of the present invention will be described in relation to system 10 as shown in Figure 1 and the flowchart diagram of Figure 2.

This conditional access system is based on authentication of each device (for example, SC 30 and SP 40) communicating with STB 20 prior to establishing a communication channel between a STB 20 and SP 40. Particularly, this conditional access system utilizes an asymmetric key system (i.e., public-key system), wherein only public keys are stored in the set-top box. That is, the set-top box does not store or contain any secrets (i.e., private keys). The foundation of public-key cryptography is the use of two related keys, one public

and one private; the private key being computationally unfeasible of being deduced from the public key which is publicly available. Anyone with a public key can encrypt a message but only the person or device having the associated and predetermined private key can decrypt it. Similarly, a message can be encrypted by a private key and anyone with access to the public key can decrypt that message. Encrypting messages using a private key may be referred to as "signing" because anyone holding the public key can verify that the message was sent by the party having the private key. This may be thought of as being analogous to verifying a signature on a document.

A digital certificate or certificate is a message sent in the clear (i.e., unencrypted) having a CA 50 signature attached thereto; thus the recipient of the certificate can verify the source or origin of the certificate. These digital certificates are in fact "signed messages" because the signature attached to the message is produced by encrypting either the message itself or a digest of the message (which is obtained by hashing the message, as described later). Unilateral authentication of each device connected to the set-top box is achieved by passing such certificates between the devices and verifying these certificates. Certificate verification involves checking the signature by decryption. These certificates may contain information used by the device receiving the certificate. This information may be related to a device not involved in the passing of this certificate, e.g. information contained in the first digital certificate is related to the service provider as described below. Further, the certificates may contain information associated with the device passing the certificate and a public key of the passing device.

As described above, only public keys are stored in a memory device contained in STB 20. Further, the first and second digital certificates, which may be issued by CA 50, are stored in SC 30 and SP 40, respectively.

The following nomenclature will be utilized in the below description of the present conditional access system.

KCApri1	Private key used to create SC's certificate
KCApub1	Public key used to verify SC's certificate
KCApri2	Private key used to create SP's certificate
KCApub2	Public key used to verify SP's certificate
KSPpub	SP's Public key
KSPpri	SP's Private key

These are used and discussed with respect to authenticating a device such as the smart card or the service provider.

After STB 20 is activated and SC 30 is inserted into STB 20, STB 20 sends a first message to SC 30 (see Figure 2, Step 100). This first message contains identification data corresponding to STB 20, for example, such identification data may include the manufacturer's identification data (MID). In response to the first message, SC 30 replies by sending a first digital certificate back to STB 20 (see Figure 2, Step 120). The first digital certificate (i.e., SC's certificate) includes data sent in the clear and an attached signature which is encrypted using KCApri1, the private key which is used to create certificates sent by SC 30. This data may include identification

data corresponding to a selected service provider having a pre-existing agreement with the manufacturer of STB 20. Particularly, this data may also include, in addition to the service provider identification data, a phone number for the service provider which will be used for contacting the service provider as described below.

If SC 30 does not have a digital certificate associated with a service provider (see Figure 2, Step 110), STB 20 may contact an independent party (not shown), download an appropriate digital certificates from the independent party (see Figure 2, Step 114) and transfer them to SC 30 (see Figure 2, Step 116). STB 20 may contact the independent party utilizing an integrated modem. If the digital certificates are downloaded from the independent party, the above process may continue starting at the point where SC 30 replies to the first message by sending a first digital certificate back to STB 20.

Now, STB 20 must authenticate (see Figure 2, Step 130) SC 30 by verifying that SC 30 has passed a valid certificate to STB 20, this involves decrypting the first digital certificate in STB 20 using KCApub1. KCApub1, which is stored in STB 20, is the corresponding public key also assigned by CA 50. After SC 30 is authenticated, the service provider identification data included in the first digital certificate is used by STB 20 to contact the desired service provider, for example SP 40.

SC 30 may have more than one digital certificate, each one of which may identify a different service provider. If this is the case, the user may be prompted to select one of the service providers having a valid certificate (see Figure 2, Step 140). Further, if a

service provider has more than one access number, the set-top box may select an alternate number if, for example, the primary number is busy.

STB 20 sends a second message to SP 40 (see Figure 2, Step 150); this second message contains similar identification data corresponding to STB 20. For example, such identification data now may include the manufacturer's identification data (MID) and a date and time stamp (DTS). DTS may be downloaded from an electronic program guide or from a special time server or possible through an internal means. In response to the second message, SP 40 replies by sending (1) a second digital certificate (i.e., SP's certificate) and (2) the second message encrypted using KSPpri back to STB 20 (see Figure 2, Step 160). The second digital certificate includes data sent in the clear and an attached signature which is created using KCApri2. This data may include identification data corresponding to the service provider, the validity period (VP) for the second digital certificate and the public key for SP 40, i.e., KSPpub. The identification data may also further include data associated with CA 50 which may be utilized, if necessary, for authentication of SP 40. Now SP 40 must be authenticated; such authentication is achieved utilizing the second digital certificate and the encrypted second message (see Figure 2, Step 170).

Particularly, authentication of the service provider involves (1) decrypting the second digital certificate in STB 20 using KCApub2, which is stored therein, (2) decrypting the encrypted second message using the public key of SP 40 (i.e., KSPpub) which is included in the second digital certificate and (3) comparing the

decrypted "encrypted second message" to the original second message sent to SP 40. This ensures that the certificate was received from the desired service provider and not from another source.

Further, the data contained in the second digital certificate may be subjected to a one-way hashing algorithm, such as MD5 developed by Ron Rivest or SHA-1 developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) prior to being encrypted by KCApri2. If this is the case, authentication may also include hashing the data sent in the clear using the same one-way hashing algorithm and comparing this data to the decrypted data. Similarly, the creation of the first digital certificate may involve the use of such a one-way hashing algorithm.

After SP 40 has been authenticated by STB 20, STB 20 sends confirmation of this authentication back to SP 40 (see Figure 2, Step 180). This confirmation involves sending the second message now being encrypted using the public key of SP 40, i.e., KSPpub, back to SP 40. SP 40 can decrypt this message using its associated private key, KSPpri. Finally, STB 20 establishes a communication channel (see Figure 2, Step 190) between STB 20 and SP 40 wherein all future communication may be handled utilizing public-key cryptography and the public and private key pairs associated with SP 40 (i.e. KSPpub and KSPpri).

The present invention has been described in terms of an exemplary embodiment in which a single smart card cooperates with a single set-top box to manage access to a single service provider. However, it is within the scope of this invention to provide a

conditional access system which may be extended to permit the smart card to "roam" across (i.e., provide conditional access between) multiple service providers and multiple manufacturers of the set-top boxes. This is particularly illustrated in Figure 3 where SC 30a may be used in any one of STBs 20a, 20b or 20c to access any one of SPs 40a, 40b or 40c. In such a system, each set-top box manufacturer will have a unique MID. The smart card will have a unique first digital certificate for each service provider and for each manufacturer having a predetermined agreement with the service provider. Each set-top box will have unique sets of public keys for verifying these digital certificates. For example, if there are "m" service providers and "n" manufacturers of set-top boxes then the smart card may contain up to "m times n" number of digital certificates.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon a reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims. Further, it is within the scope of the present invention that the conditional access system defined herein is fully capable of being utilized between any two devices interconnected.

Claims

1. A method for managing access to a device, said method comprising:

(a) sending a first message from a first device to a second device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device;

(c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device;

(d) authenticating said second device in response to said digital certificate and said first encrypted message; and

(e) establishing a communication channel between said first and said second devices in response to the authentication of said second device.

2. The method of Claim 1 wherein said first message comprises first identification data associated with said first device and a date and time stamp.

3. The method of Claim 2 wherein said digital certificate comprises second identification data associated with said second device and a second public key of said second device.

4. The method of Claim 3 wherein the step of authenticating comprises the steps of:

(a) decrypting said digital certificate in said first device using a first public key;

(b) decrypting said first encrypted message using said second public key to generate a first decrypted message; and

(c) comparing said first decrypted message to said first message.

5. The method of Claim 4 wherein said first public key is stored in said first device.

6. The method of Claim 5 further comprising the step of providing confirmation of the authentication to said second device by

(a) encrypting said first message using said second public key to generate a second encrypted message; and

(b) sending said second encrypted message to said second device.

7. The method of Claim 6 wherein said digital certificate, said first public key and said first private key are issued by an independent certificate authority and are associated with said second device.

8. The method of Claim 1 wherein said first device is a set-top box and said second device is a server associated with a service provider.

9. The method of Claim 8 wherein said second identification data further comprises data associated with said certificate authority and data associated with the validity of said digital certificate.

10. A method for managing access to a device, said method comprising:

(a) sending first identification data associated with a first device to a second device;

(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device;

(c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving, in said first device, from said second device said first encrypted identification data;

(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;

(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;

(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;

(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and

(i) establishing a communication channel between said first and said second devices.

11. A system for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:

(a) sending a first message to the smart card, said first message containing set-top box identification data;

(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;

(c) authenticating the smart card in response to said first digital certificate;

(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

12. The system of Claim 11 wherein the smart card comprises a plurality of digital certificates, each one containing service provider identification data associated with a unique service provider.

13. The system of Claim 12 wherein the step of authenticating the smart card in response to said first digital certificate comprises decrypting said first digital certificate in said set-top box using a first public key.

14. The system of Claim 13 wherein said second digital certificate comprises second service provider identification data and a second public key of said service provider.

15. The system of Claim 14 wherein the step of authenticating the service provider comprises the steps of:

(a) decrypting said second digital certificate in the set-top box using said second public key;

(b) decrypting said encrypted second message using a third public key to generate a second decrypted message; and

(c) comparing said second decrypted message to said second message.

16. The system of Claim 15 wherein said first public key, said second public key, said first message and said second message are stored in said set-top box.

17. The system of Claim 16 wherein said first digital certificate, said first private key and said first public key are issued by an independent certificate authority.

18. The system of Claim 17 wherein said first digital certificate is stored in said smart card.

19. The system of Claim 18 wherein said second digital certificate, said second private key and said second public key are issued by an independent certificate authority and are associated with said service provider.

20. The system of Claim 19 wherein said second digital certificate is stored in said service provider.

Abstract of the Disclosure

A system conditionally establishes a communication channel between two devices only if one device is authenticated by the other device. Authentication of the second device by the first device involves sending a message to the second device; receiving, from the second device, the message encrypted using a private key of the second device and a digital certificate having a public key of the second device; decrypting the digital certificate to obtain the public key, using the public key to decrypt the message and comparing the decrypted message to the message originally sent to the second device.

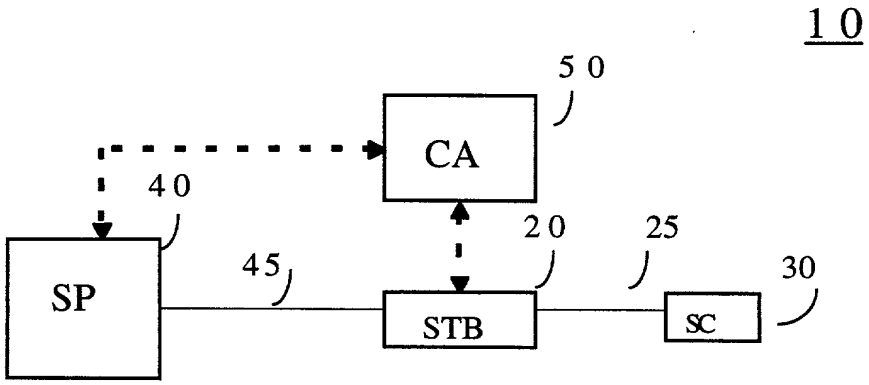

Fig 1.

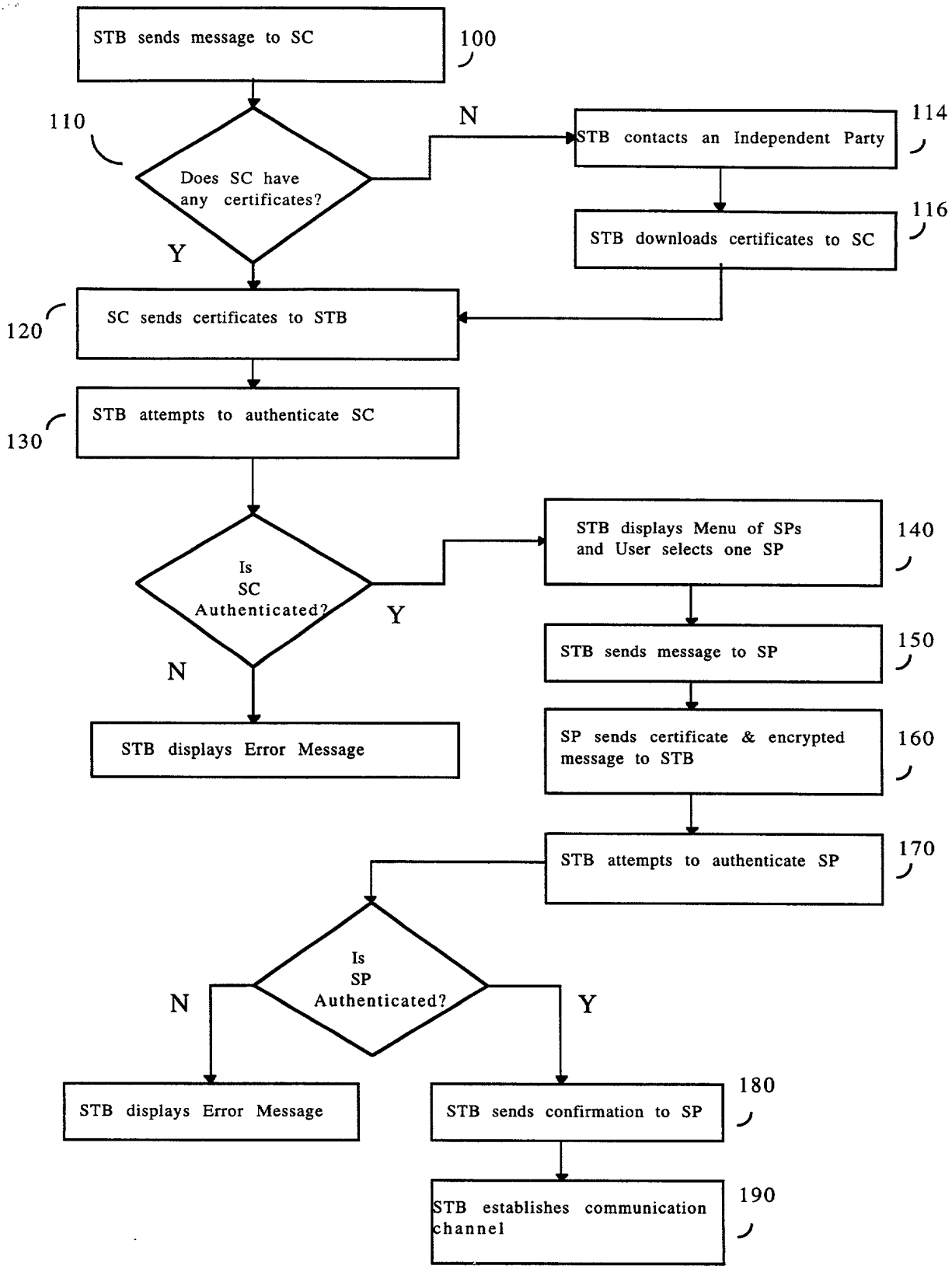
STB sends message to SC
100
110
Does SC have any certificates?
N
STB contacts an Independent Party
114
STB downloads certificates to SC
116
Y
SC sends certificates to STB
120
STB attempts to authenticate SC
130
Is SC Authenticated?
Y
N
STB displays Menu of SPs and User selects one SP
140
STB sends message to SP
150
STB displays Error Message
SP sends certificate & encrypted message to STB
160
STB attempts to authenticate SP
170
Is SP Authenticated?
N
Y
STB displays Error Message
STB sends confirmation to SP
180
STB establishes communication channel
190

Fig 2.

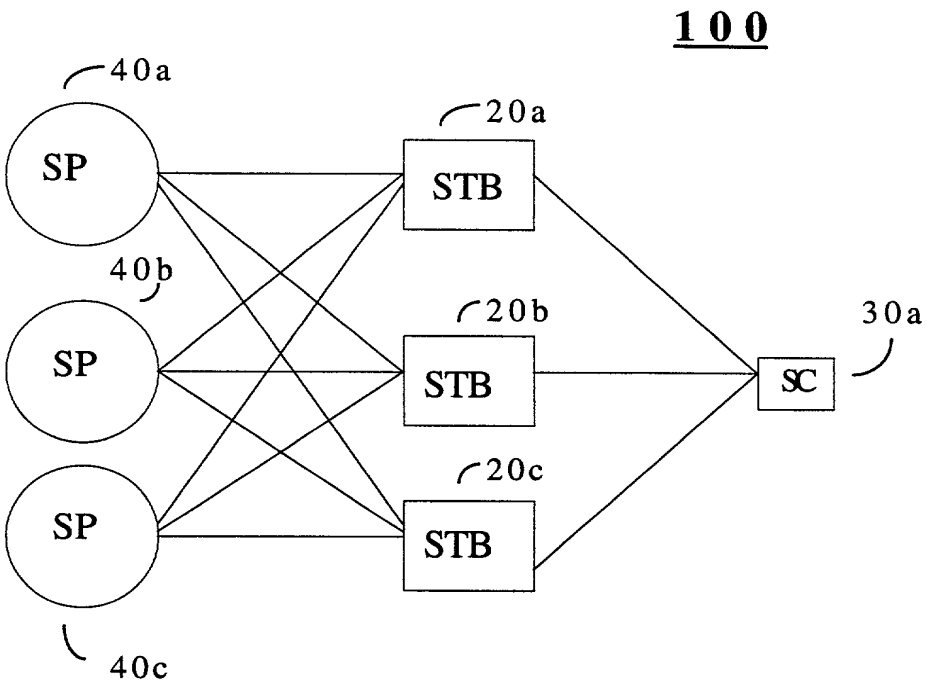

Fig. 3

RCA 88,637

DECLARATION AND POWERS OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES**
the specification of which was filed on **12/3/99** as Application Serial No. **09/445,132** and was amended on _____
or, if not identified here by filing date and serial number, is attached hereto.

I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 USC 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate by me or my representatives or assigns for this invention having a filing date before that of the application on which priority is claimed.

Application No. _____ in _____ on _____ priority claimed [ ] Yes [ ] No
Application No. _____ in _____ on _____ priority claimed [ ] Yes [ ] No

I hereby claim the benefit under 35 USC 119(e) of any United States provisional application(s) as listed below.

Application No. **60/048,852** Filed **June 6, 1997**
Application No. _____ Filed _____

I hereby claim the benefit under 35 USC 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose material information as defined in 37 CFR 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application

Serial No. PCT/US98/11634 Filed 6/5/98 [ ] patented [X] pending [ ] abandoned

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint, individually and collectively, the following as my/our attorney or agent with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith:

3

Joseph S. Tripoli Registration No. 26,040 and
Robert D. Shedd Registration No. 36,269 and
David T. Shoneman Registration No. 39,371

PLEASE ADDRESS ALL
COMMUNICATIONS TO: **JOSEPH S. TRIPOLI**
PATENT OPERATIONS
THOMSON MULTIMEDIA LICENSING, INC.
P. O. Box 5312
PRINCETON, NEW JERSEY 08543-5312

Sole or Joint Inventor (1)	Ahmet Mursit Eskicioglu (Type or Print)	Ahmet Mursit Eskicioglu (Signature in Full. No initials.)
Citizenship	Turkey	Date 3/6/00
Post Office Address	8235 Lakeshore Trail No. 125, Indianapolis, IN 46250, USA	IN
Residence	Same as above	
Sole or Joint Inventor (2)	Keith Reynolds Wehmeyer (Type or Print)	Keith Reynolds Wehmeyer (Signature in Full. No initials.)
Citizenship	USA	Date 3/6/00
Post Office Address	6411 Columbia Circle, Fishers, IN 46038 USA	IN
Residence	Same as above	
Sole or Joint Inventor (3)	David Emery Virag (Type or Print)	David Emery Virag (Signature in Full. No initials.)
Citizenship	USA	Date 3-6-00
Post Office Address	7485 Cherry Hill Drive, Indianapolis, IN 46254 USA	IN
Residence	Same as above	